

On Tradeoffs between Trust Accuracy and Resource Consumption in Communications and Social Networks

Jin-Hee Cho, Kevin Chan, Ananthram Swami, Brian Rivera

US Army Research Laboratory

{jinhee.cho, kevin.s.chan, ananthram.swami, brian.rivera1}@us.army.mil

Summary

Managing trust efficiently and effectively is critical in tactical networks in order to facilitate cooperation and decision making tasks as well as to meet system goals such as reliability, availability and scalability [1]. The accuracy of evaluated trust values may significantly affect mission performance. However, acquiring evidence to evaluate trust accurately can require significant resources (such as bandwidth, time and energy) that are often severely constrained in mobile ad hoc networks (MANETs). We study this tradeoff in a framework that balances the accuracy of evaluated trust with resource consumption.

Our goal is to develop a general trust management framework that minimizes resource consumption (e.g., communication overhead for trust formation, aggregation, and propagation) while obtaining accurate measures of trust by entities. In particular, we investigate the impact of trust chain length, the use of indirect information to establish trust values, and the impact of misbehaving nodes on both communication overhead and the accuracy of evaluated trust relationships.

Trust relationships involve the interaction of two nodes: a trustor (evaluator) and trustee (entity being evaluated). We consider the impact of misbehaving (selfish or malicious) nodes on the evaluation of trust. We also consider the interaction between network dynamics (changing network topology) and trust. We have developed Markov models for the evolution of trust and have analytically validated our theoretical results via simulations using Stochastic Petri Nets (SPN).

We use a social networking experimental platform called ELICIT to experimentally validate the interactions and parameter trades in communications and social networks. Based on our analytical and empirical results, system designers in tactical networks can adjust key design parameters (e.g., length of a trust chain, amount of recommendations) to meet both trust accuracy and resource consumption objectives.

Composite Trust Metric

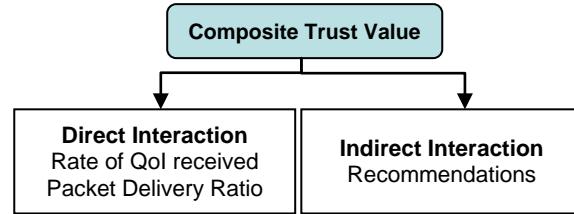


Fig. 1: Composite trust metric.

We use both direct and indirect information to derive trust of an entity. First, as Fig. 1 explains, a trust value is based on direct observations about quality of service (e.g., packet delivery ratio) or quality of information (e.g., data integrity or data relevance) [2]. Second, to increase trust accuracy, we use third party recommendations to provide indirect information. In particular, direct observers of a trustee can be candidates to provide useful trust-related information on that node and are called functional trust recommenders [2]. The cooperation of multiple intermediate entities is required for the delivery of trust information about the trustee if it is located far away a trustor. These intermediate entities or relays are called referral trust recommenders since they only pass the trust information to the trustor. We

consider the dynamics of trust in tactical environments.

Trust decays when there are no recent updates or interactions between a trustor and trustee. We also use the concept of the *web of trust*, implying the “weighted transitivity” of trust. For example, when A trusts B, B trusts C, and C trusts D, A may use the A-B, B-C, and C-D trust relationships to derive the A-D trust relationship. Jøsang’s algebra [2] is applied to derive trust using a trust chain (TC). If no trust information is available at current time t , then trust is derived based on the trustor’s past experience with the trustee.

Trust in Communication Networks

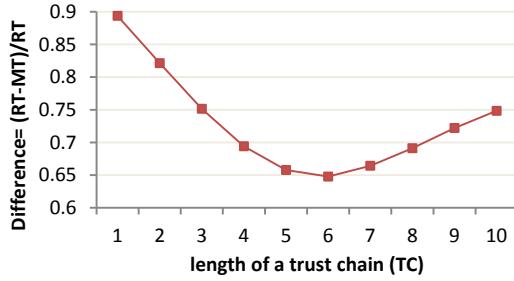


Fig. 2: Trust accuracy vs. trust chain length;
RT-real trust; MT-measured trust.

We show our preliminary results on the overhead-accuracy trades through the evaluation of our Markov models. Fig. 2 shows that there exists an optimal trust chain with respect to the accuracy of the computed trust value (TC = 6). As TC length increases, the probability of receiving trust information increases. However, once the trust chain is greater than 6, the security vulnerability caused by requiring more intermediate nodes to pass trust information and the spatial or temporal decay of trust outweigh the gains of having more information.

Fig. 3 shows that the communication overhead for trust evaluation increases linearly as the length of the trust chain increases. However, when energy, collision and interference constraints are taken into account, the

relationship will be nonlinear, as we shall show in the full paper.

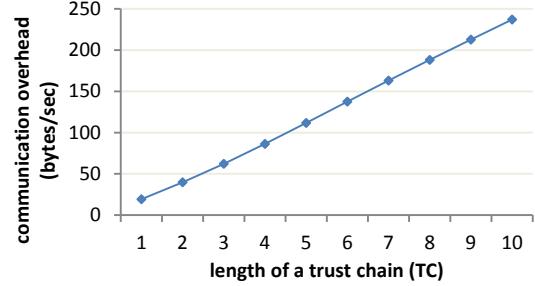


Fig. 3: Overhead vs. trust chain length.

Trust in Social Networks

Trust relationships are inherent aspects of social networks, but characterizing the cognitive and sociological effects is a very complex problem. Elements of trust relationship dynamics in the communication network context can be adapted to social networks. Specifically, trust management is considered in the context of an information gathering task, where a social network is overlaid on a communication network. Trust relationships are modeled with respect to network quality of service and the behavior of neighboring nodes. Further, the tradeoff between communication overhead and trust accuracy is studied. Experimental results using ELICIT [3] will be reported in the full paper.

Conclusion

This work examines the tradeoff between trust accuracy and resource consumption when establishing trust levels in both communications and social networks. Our full paper will include details of sensitivity analysis under various key design parameters in order to identify optimal settings to meet both trust accuracy and performance goals.

References

- [1] D.C. Arney and E. Peterson, Proc. Army Science Conf., 2008.
- [2] A. Jøsang, Proc. Network and Distributed Systems Security (NDSS’99) Symp., 1999.
- [3] M. Ruddy, 12th Int’l Command and Control Research and Technology Symp., June 2007.